UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/695,837	10/30/2003	Tzahi Carmeli	P-5763-US	7206

49444 7590 06/14/2007

PEARL COHEN ZEDEK LATZER, LLP
1500 BROADWAY, 12TH FLOOR
NEW YORK, NY 10036

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
06/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/695,837	CARMELI, TZAHI	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19 and 26-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19 and 26-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on March 28, 2007. Claims **20-25** are canceled. No new claims are added. Claims **1, 3, 4, 6 and 32-36** are amended. **Claims 1-19 and 26-36 are pending/examined.**

Response to Arguments

2. Applicant's remark/arguments filed on March 28, 2007 have been fully considered but they are not persuasive.

Applicant argument is based on the reference used in rejecting the corresponding limitation recited in the independent claims 1, 12, 26 and 32. Applicant in particular argued that the limitations which is recited in the amended claim 1, such as "if the header indicates transmitting, configuring transmitter to encrypt the data frame; and

If the header indicates receiving configuring a receiver to decrypt the data frame" is not disclosed by the reference on the record.

For instance in order to support his argument, Applicant wrote the following.

"The Office Action rejected Claims 1-36 under 35 U.S.C. § 102(b) as being anticipated by Callum, U.S. Patent No. 6,295,604.

Independent Claims I and 32, as currently amended, recite, inter alia, "'configuring a transmitter to encrypt the data frame" and "configuring a receiver to decrypt the data frame." Callum does not disclose these features. Callum's disclosure of a "CPP [cryptographic packet processing] unit to perform encryption and decryption operations" (Callum, column 3, lines 32-33) does not describe the transmitter and receiver of Claims 1 and 32.

Each of independent claims 12 and 26 recites, inter alia, "'a configuration unit to configure the transmitter and the receiver base on information included in the data

frame." Callum does not teach or suggest "a configuration unit to configure the transmitter and the receiver" as recited in independent claims 2 and 26. Therefore, Applicant respectfully submits that Claims 1, 12, 26 and 32 are not anticipated by Callum."

Examiner disagrees with the above argument.

Examiner would point out that "transmitter" and "receiver" are terms the can be used for one and the same device. For instance, a client can receive or transmit data. By the same token a server can also receive and transmit data. Therefore, unless it is specifically indicated in the claim itself that the transmitter and the receiver are two different entities separated from each other, examiner interpretation of the cryptographic unit shown on figure 2, ref. Num 250 as both a transmitter and receiver is a correct interpretation.

Furthermore, as far the claim language is concerned what makes the transmitter a transmitter is nothing but encrypting the data frame and what makes a receiver a receiver is nothing but being capable of decrypting the data frame and both functions, encryption/decryption is done based on the information indicated by the header.

And this is undoubtedly disclosed by at the reference on the record namely *Callum.*

Examiner would point that Callum on column 3, lines 18-24 discloses that Memory controller 220 controls (i) the retrieval of a data packet from memory unit 210, and (ii) the storage of digital information within memory unit 210. **CPP unit 230 comprises a packet controller 240** and **a cryptographic unit 250**. **Packet controller 240 receives a data packet from memory controller 220, separates the control information in its header from the data portion**, and **separately transmits this information across signal lines 260 and 270, respectively. Cryptographic unit 250 encrypts or decrypts the contents of**

the data portion in accordance with the control information provided by the header.

In order to show how each and every limitations of the independent claims is disclosed by the reference on the record namely *Callum, Examiner would show the following.*

Referring to the independent claims 1, 12, 26 and 32, Callum the reference on the record discloses the following.

A method comprising:

- **Receiving a date frame comprising a header and a data portion.***[Column 5, lines 17-2] (Packet controller 240 receives a data packet from memory controller 220, and this data packet is comprises of a header having a control information and data portion and the packet controller 240 then separates the control information in its header from the data portion)*
- **If the header indicates transmitting, configuring transmitter to encrypt the data frame [Column 5, lines 17-24]** *(Packet controller 240 separately transmits this header information across signal lines 260 and 270, respectively. Cryptographic unit 250 which is interpreted as the transmitter/receiver encrypts the contents of the data portion in accordance with the control information provided by the header, implies that if the header information indicates encryption then the cryptographic unit 250 encrypts the data and inherently transmit the encrypted data/cipher) and;*

- **If the header indicates receiving configuring a receiver to decrypt the data frame [Column 5, lines 17-24]** *(Packet controller 240 separately transmits this header information across signal lines 260 and 270, respectively. Cryptographic unit 250 which is interpreted as the transmitter/receiver decrypts the contents of the data portion in accordance with the control information*

provided by the header, implies that if the header information indicates decryption then the cryptographic unit 250/receiver decrypts the data)

Since the rest of the Applicant's argument is based on the above argument, examiner's reasons provided above is also applicable towards the rest of applicant's argument.

The last argument presented by the applicant is towards the dependent claims.

Examiner disagrees with the argument as the dependent claims stands and falls with the corresponding independent claims.

Therefore all limitations recited in the independent claims are undoubtedly disclosed by the reference/s on the record and the rejection is maintained until the applicant amends the independent claims and successfully overcome the rejection without introducing new matters.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. **Claims 1-36** are also rejected under 35 U.S.C. 102(b) as being anticipated by **Callum** (Hereinafter referred as **Callum)** (U.S. Patent No. 6,295,604, Patent Date September 25, 2001)

5. As per independent claims 1, 12, 26 and 32 Callum discloses a method comprising:

- **Receiving a date frame comprising a header and a data portion**.*[Column 5, lines 17-2] (Packet controller 240 receives a data packet from*

memory controller 220, and this data packet is comprises of a header having a control information and data portion and the packet controller 240 then separates the control information in its header from the data portion)

- **If the header indicates transmitting, configuring transmitter to encrypt the data frame [Column 5, lines 17-24]** *(Packet controller 240 separately transmits this header information across signal lines 260 and 270, respectively. Cryptographic unit 250 which is interpreted as the transmitter/receiver encrypts the contents of the data portion in accordance with the control information provided by the header, implies that if the header information indicates encryption then the cryptographic unit 250 encrypts the data and inherently transmit the encrypted data/cipher) and;*

- **If the header indicates receiving configuring a receiver to decrypt the data frame [Column 5, lines 17-24]** *(Packet controller 240 separately transmits this header information across signal lines 260 and 270, respectively. Cryptographic unit 250 which is interpreted as the transmitter/receiver decrypts the contents of the data portion in accordance with the control information provided by the header, implies that if the header information indicates decryption then the cryptographic unit 250/receiver decrypts the data)*

6. **As per claims 2-3, 13-14, 27-28 and 33-34 Callum discloses a method as applied to claims above. Furthermore, Callum discloses the method further comprising authenticating the header of the data frame and processing the header of the data frame to provide a processed header; and configuring the transmitter and the receiver based on information included in the processed header.** [See figure 3-5 and at least column 3, lines 25-column 4, line 10]

7. As per claims 4-11, 15-19, 29-31 and 35-36 Callum discloses a method as applied to claims above. Furthermore, Callum discloses the method wherein configuring comprises: configuring the receiver to authenticate and decrypt a data portion and a message integrity code portion of the data frame. [figure 3-5] **and the method further comprising: decrypting the data portion and the message integrity code portion of the data frame to provide a decrypted data portion and a decrypted message integrity code portion, respectively; calculating the message integrity code of the data frame from the decrypted data portion; and comparing the calculated message integrity code to the decrypted message integrity code portion.** [See figure 3-5 and at least column 3, lines 25-column 4, line 10] (Referring now to FIGS. 3-5, data packet 300 includes a header 310 and a data portion 350. In this embodiment, header 310 comprises control information including a control word 320, one or more keys 330 and an initialization vector (IV) 340 as shown in FIG. 4. Control word 320 provides information to control the functionality of CPP unit 230 of FIG. 2. The keys 330 and IV 340 are used by CPP unit 230 to perform encryption or decryption operations. And As shown in FIG. 5, one embodiment of control word 320 includes a plurality of bit fields 321-324. These bit fields 321-324 provide the CPP unit with information concerning the length of data packet 300 of FIG. 3, the mode of operation (encryption/decryption), and optionally, the type of cryptographic technique used. It is contemplated that different bit lengths associated bit fields 321-324 may be utilized other than the bit lengths illustrated herein. In particular, as shown in FIGS. 3 and 5, first bit field 321 contains a byte count which indicates the number of bytes in data packet 300, and second bit field 322 includes one or more bits which indicate whether encryption or decryption is to be performed on data portion 350 of the incoming data packet. As optional bit fields of control word 320, third/forth bit fields 323 and 324 indicate the type of cryptographic operation to be performed. For example, if the CPP unit supports DES, third bit field 323 may indicate a selected DES mode (e.g., triple key DES) and fourth bit field 324 may indicate whether Cipher Block

Chaining (CBC) or Electronic Codebook (ECB) is desired. The operations associated with CBC and ECB are set forth in a Federal Information Processing Standard Publication (FIPS Pub. 81) entitled "DES Modes of Operation" published on or around Dec. 2, 1980. It is contemplated that other types of cryptographic operations would assign bit fields 323 and 324 to provide different information. Referring back to FIGS. 2 and 4, header 310 further includes keys 330 and IV 340. In this embodiment, three (3) keys are provided, each key being at least 56-bits in length, although any bit size may be used so long as it is in accordance to the cryptographic standard followed by CPP unit 230. In the event that a 32-bit data bus is implemented between memory controller 220 and CPP unit 230, two data transfers maybe employed, in this embodiment to transfer one of the keys 330 as shown in FIG. 4. Initialization vector (IV) 340 is a binary vector used as a randomizing block of data that is exclusively OR'ed (XOR) with a first data block in CBC mode. Finally the following has been disclosed, "Referring back to FIG. 3, data portion 350 includes N data blocks 360.sub.1 -360.sub.N, where "N" is a positive whole number. In this embodiment, a "block" is a 32-bit word. The sizing of the word is constrained by the bit width of the cryptographic bus situated between memory controller 220 and CPP unit 230 of FIG. 2.")

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
06/02/2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER